WEBERNETZ.NET
NETWORK SECURITY CONSULTING

Incorrect Working IPv6 Clients/Networks on the Internet

Johannes Weber

Webernetz.net – Network Security Consulting

#whoami: Johannes Weber

- Senior Security Engineer
  @ TÜV Rheinland i-sec GmbH
  - Firewalls
  - VPN/Crypto
  - Routing/Switching
- IPv6
- DNSSEC
- NTP

- https://weberblog.net
- @webernetz

Agenda

- ICMPv6 Basics
- Case Study: NTP Pool
- ~~Using Wireshark/tshark~~
- ~~Strange things~~

Motivation

- Investigate, whether or not it‘s your fault!
- (If any…)

ICMPv6 Basics

Photo by Jonas Jacobsson on Unsplash

ICMPv6 Destination Unreachable = Type 1

- Code 0: no route to destination
  - only in the default-free zone (without default routes)
  - c->s: typing error, false AAAA record
  - s->c: spoofed source address

- Code 1: communication with destination administratively prohibited
  - aka firewall
  - c->s: normal firewall behaviour
  - s->c: missing stateful firewall?!?

ICMPv6 Destination Unreachable = Type 1

- Code 2: beyond scope of source address
  - has someone ever worked with scopes other than link-local and global?

- Code 3: address unreachable
  - layer 2 address not resolvable, NS sent but INCOMPLETE
  - c->s: link down, wrong address, false AAAA record
  - s->c: link down, spoofed source address

ICMPv6 Destination Unreachable = Type 1

- Code 4: port unreachable
  - if transport protocol has no listener
  - that is: UDP
  - (TCP has RST)
  - c->s: server isn‘t listening, port scan [1]
  - s->c: client has closed source port too early
  - heavily realted to defective NTP clients [2]

[1] https://weberblog.net/nmap-packet-capture/

[2] https://www.linkedin.com/pulse/how-use-ntp-pool-heiko-gerstung/

Case Study: NTP Pool

Case Study: NTP Pool

- Dynamic collection of volunteer NTP servers
- Default „time server“ for many Linux distributions and network devices (routers, IoT, …)
- Meinberg M200 appliance w/ DCF77
- IPv6-only: `ntp3.weberlab.de` `ntp3-legacy-ip.weberlab.de`

Case Study: NTP Pool

	IPv6	Legacy IP
Number of NTP packets	7 M	85 M
NTP packets per second	1.24	14.9
Unique source addresses of NTP packets	0.65 M (9.3 %)	3.4 M (4 %)
NTP sources that caused ICMP errors	30 K	96 K
Percentage of failed NTP sources	**4.55 %**	**2.81 %**

- Each IPv6 source address == unique NTP client
- NOT true for legacy IP

Case Study: NTP Pool

Distribution of ICMP Errors	IPv6	Legacy IP
dest unreach, no route to dest [net unreach]	1.63 %	0.15 %
dest unreach, administrat prohibited [diverse]	0.31 %	0.14 %
dest unreach, address unreach [host unreach]	**87.51 %**	1.42 %
dest unreach, port unreach	9.82 %	**98.28 %**
time exceeded	0.73 %	0.02 %

- Uh, almost **88 %** of errors are address unreachable -> **ND problem**
- (Or address spoofing?)

Case Study: NTP Pool

Distribution of NTP Clients	Sources	Sources with Address Unreachable	Without Address Unreachable
All clients	657 K	26 K	96.07 %
/64 networks	640 K	25 K	96.05 %
/48 networks	178 K	20 K	**88.6 %**
/32 networks	1.9 K	0.6 K	**67.76 %**

- Mostly only 1 client per /64
- /48 boundaries: **11.4 % have at least 1x address unreachable**
- /32 boundaries: **32.2 % have at least 1x address unreachable**

Conclusion

Photo by Thought Catalog on Unsplash

Conclusion

- ICMP provides useful information
- Analysis requires special tools & tricks
- NTP Pool case study:
  - 4.55 % failed IPv6 NTP sourcse vs. 2.81 % legacy IP
  - 88 % of failed IPv6 sources: address unreachables -> ND problem
- Recommendation: capture & analyse on a regular basis

Sources & Further Reading

- „Internet Control Message Protocol“ <- fun fact: I haven‘t said it yet
- Shichao‘s Notes, ICMPv4 and ICMPv6: Internet Control Message Protocol: https://notes.shichao.io/tcpv1/ch8/
- O‘Reilly, IPv6 Essentials by Silvia Hagen: https://www.oreilly.com/library/view/ipv6-essentials/0596001258/ch04s02.html
- RFC 4443, Internet Control Message Protocol (ICMPv6): https://tools.ietf.org/html/rfc4443
- Weberblog.net, Incorrect Working IPv6 NTP Clients/Networks: https://weberblog.net/incorrect-working-ipv6-ntp-clients-networks/

WEBERNETZ.NET
NETWORK SECURITY CONSULTING

Questions? Comments?

johannes@webernetz.net

@webernetz

https://weberblog.net